



SonicWALL Content Filtering Service

SEGURIDAD DE RED

Solución dinámica y escalable para bloquear el contenido Web no productivo

El contenido Web inapropiado y peligroso puede llegar a su red a través de cualquier explorador instalado en su empresa. Todo contenido no filtrado puede introducir malware en la red, reducir la productividad y exponer a la empresa a riesgos como el incumplimiento de normas, la denegación de fondos de fomento e incluso la responsabilidad penal. Por ejemplo, en EEUU, las escuelas y bibliotecas que se benefician del programa eRate están obligadas por ley a instalar una solución de filtrado de contenido de acuerdo con la ley CIPA (Children's Internet Protection Act).

SonicWALL® Content Filtering Service (CFS) ofrece una solución de filtrado de contenido sin igual para empresas, instituciones educativas, bibliotecas, agencias gubernamentales, y terminales de Internet públicos. Pensada para organizaciones de todos los tamaños, SonicWALL CFS bloquea el contenido inapropiado, reduce el riesgo de responsabilidad legal e incrementa la productividad. Para ello, utiliza una completa base de datos con millones de URLs, direcciones IP y sitios Web. Gracias a su arquitectura de clasificación y caché de alto rendimiento, CFS actualiza las clasificaciones automáticamente de forma local en un dispositivo de seguridad de red SonicWALL para poder realizar una comparación instantánea. Con CFS, los administradores pueden aplicar políticas de acceso o bloqueo basándose en más de 56 categorías de URL, la identidad del individuo o grupo, o la hora del día.

Prestaciones y ventajas

Filtrado granular de contenido. Permite al administrador bloquear todas las categorías predefinidas, o cualquier combinación de categorías, y aplicar estas políticas a nivel granular. La autenticación a nivel de usuario (ULA) y el inicio de sesión único (SSO) pueden utilizarse para imponer el inicio de sesión mediante nombre de usuario y contraseña. CFS es capaz de bloquear el contenido potencialmente peligroso, como Java,™ ActiveX,® y Cookies, así como de programar el filtrado según la hora del día, (p.ej., durante el horario escolar o comercial). Además, CFS mejora el rendimiento, ya que elimina las aplicaciones de mensajería instantánea y MP3, los flujos de datos multimedia, el freeware y otros archivos con un consumo elevado de ancho de banda.

Arquitectura de clasificación actualizada dinámicamente. Compara las páginas Web solicitadas con una base de datos de alta precisión que incluye millones de URLs, direcciones IP y dominios. El dispositivo SonicWALL recibe clasificaciones en tiempo real, y las compara con las políticas de seguridad locales. A continuación, el dispositivo acepta o bloquea la solicitud, basándose en las políticas configuradas a nivel local por el administrador.

Cumplimiento de normas e informes. La solución soporta el cumplimiento de normas y la elaboración de informes gracias a la integración directa con el galardonado Sistema de gestión global de SonicWALL (GMS) y el paquete de informes SonicWALL ViewPoint™. En combinación con el software de informes SonicWALL ViewPoint™, SonicWALL CFS permite elaborar informes gráficos detallados o "de un vistazo" a partir de datos en tiempo real o históricos.

Gestión sencilla basada en Web. Permite configurar políticas de forma flexible y tener un control completo sobre el uso de Internet. Los administradores pueden reforzar múltiples políticas personalizadas para usuarios individuales, grupos o determinados tipos de categorías. Gracias a los filtros de URL locales, pueden aceptarse o rechazarse determinados dominios o hosts. Para bloquear el contenido dudoso con más eficacia, los administradores también pueden crear o personalizar bases de datos de filtrado.

Arquitectura de clasificación y caché de sitios Web de alto rendimiento. Permite a los administradores bloquear sitios Web de forma sencilla y automática según categorías. Las clasificaciones de URL se guardan en caché de forma local en el dispositivo SonicWALL, para que cada nuevo acceso a las páginas visitadas con frecuencia tarde tan solo una fracción de segundo.

Filtrado de contenido HTTPS basado en IP. Permite a los administradores controlar el acceso de los usuarios a las páginas Web mediante HTTPS cifrado. El filtrado HTTPS está basado en la clasificación por categorías de los tipos de páginas Web con contenido inapropiado, como p.ej., juegos de azar, banca online, compraventa de acciones online, compras, así como páginas de hackers o de puenteo de proxys.

Solución rentable y escalable. Controla el filtrado de contenido desde el dispositivo de seguridad de red SonicWALL, eliminando la necesidad de disponer de hardware adicional y evitando los gastos derivados de implementar un servidor de filtrado especial separado.

- **Filtrado granular de contenido**
- **Arquitectura de clasificación actualizada dinámicamente**
- **Cumplimiento de normas e informes**
- **Gestión sencilla basada en Web**
- **Arquitectura de clasificación y caché de sitios Web de alto rendimiento**
- **Filtrado de contenido HTTPS basado en IP**
- **Solución rentable y escalable**

Especificaciones técnicas

Arquitectura SonicWALL Content Filtering Service

Administrado mediante una interfaz intuitiva, SonicWALL Content Filtering Service (CFS) permite que tanto el filtrado como el control tengan lugar directamente en la LAN, WLAN o VPN. Al combinarse con los dispositivos de seguridad de red SonicWALL escalables y de alto rendimiento y con las eficaces prestaciones de informes y gestión del Sistema de gestión global de SonicWALL, CFS ofrece una solución de filtrado integrada, sencilla y altamente gestionable para organizaciones de todos los tamaños.



SonicWALL Content Filtering Service

Premium Business Edition para NSA E7500 (1 año)
01-SSC-7329

Premium Business Edition para NSA E6500 (1 año)
01-SSC-7330

Premium Business Edition para NSA E5500 (1 año)
01-SSC-7331

Premium Business Edition para NSA 5000 (1 año)
01-SSC-7350

Premium Business Edition para NSA 4500 (1 año)
01-SSC-7346

Premium Business Edition para NSA 3500 (1 año)
01-SSC-7333

Premium Business Edition para NSA 2400 (1 año)
01-SSC-7334

Premium Business Edition para la serie NSA 240 (1 año)
01-SSC-7335

Premium Business Edition para la serie TZ 210 (1 año)
01-SSC-7371

Premium Business Edition para la serie TZ 200 (1 año)
01-SSC-8634

Premium Business Edition para la serie TZ 100 (1 año)
01-SSC-8637

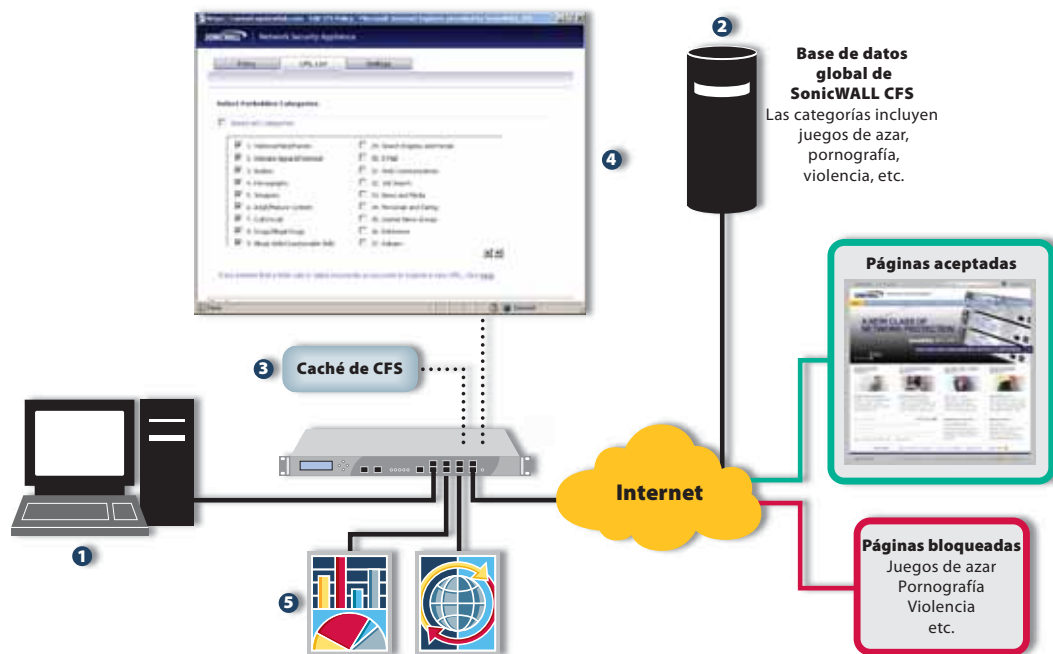
Premium Business Edition para las series TZ 180 y TZ 190 (1 año)
01-SSC-5650

Standard Edition para las series TZ 180 y TZ 190

Nodos ilimitados (1 año)
01-SSC-5505

Standard Edition para TZ 180 10/25 nodos (1 año)
01-SSC-7171

También hay disponibles números de producto para Content Filtering Service de varios años.



- 1 Usuario SonicWALL CFS
- 2 Base de datos distribuida de clasificaciones de SonicWALL CFS
- 3 Caché de clasificaciones locales de sitios aceptables
- 4 Políticas URL establecidas para bloquear los sitios Web cuestionables o contraproductivos
- 5 Informes mediante SonicWALL ViewPoint o GMS

Prestaciones	CFS Premium	CFS Standard
Categorías	56	12
Políticas usuario/grupo	Sí**	No
Clasificación dinámica	Sí	No
Informes	ViewPoint*	ViewPoint*
Caché de páginas Web	Sí	Sí
Refuerzo de búsqueda segura	Sí***	No
Refuerzo de políticas CFS por rango IP	Sí***	No

* ViewPoint se vende por separado. ** Se requiere SonicOS Enhanced. *** Requiere SonicOS 5.2 o superior.

Disponible en	CFS Premium	CFS Standard
TZ 180/180W	Sí	Sí
TZ 190/190W	Sí	Sí
TZ 100/100W	Sí	No
TZ 200/200W	Sí	No
TZ 210/210W	Sí	No
Serie NSA	Sí	No
Serie E-Class NSA	Sí	No

Si desea obtener más información sobre SonicWALL Content Filtering Service y nuestra completa línea de soluciones de seguridad, visite nuestra página Web en <http://www.sonicwall.com>.

Soporte de ventas España

Teléfono gratuito: 900.811.056

Teléfono: +31 (0) 411.617.815

Correo electrónico:

sales_support-europe@sonicwall.com

Soporte de ventas Europa

– otros países

Teléfono: +31 (0) 411.617.811

Correo electrónico:

sales_support-europe@sonicwall.com

Oficina en Portugal/España

Teléfono: +34.653.94.82.87

Correo electrónico:

spain@sonicwall.com

